네트워크 공격

00_보안공격- 보안공격이란?

❖ 보안공격(Security Attack)

- 조직의 정보보호를 저해하는 제반 행위

(IT 시스템에 정보보호를 저해하는 행위)

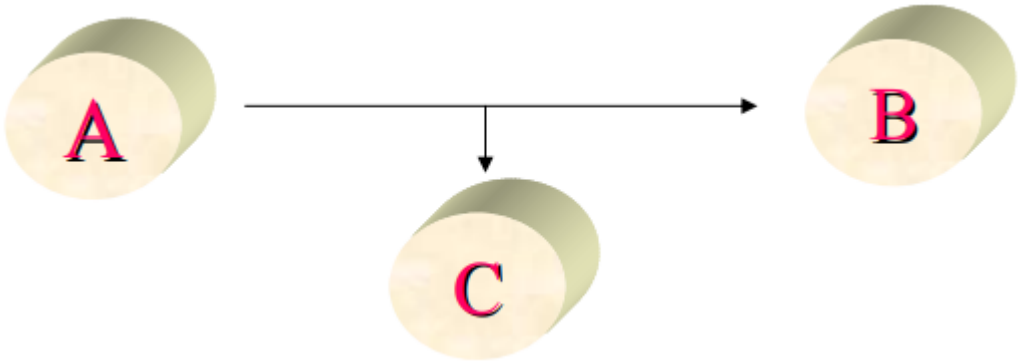
❖ 보안 공격의 유형

- 소극적 공격 (Passive Attack)
- 적극적 공격 (Active Attack)

00_보안공격- 보안공격의 유형

❖ 소극적 공격

- 전송되는 정보를 가로채서 알아내는 공격방식, 소극적 공격방식은 실제 전달되는 메시지에 아무런 변경사항이 없어 자신이 공격을 받고 있는지를 알 수가 없다.
- Ex) 도청, 가로채기, 트래픽 분석, 로그 분석 → 스니핑 등

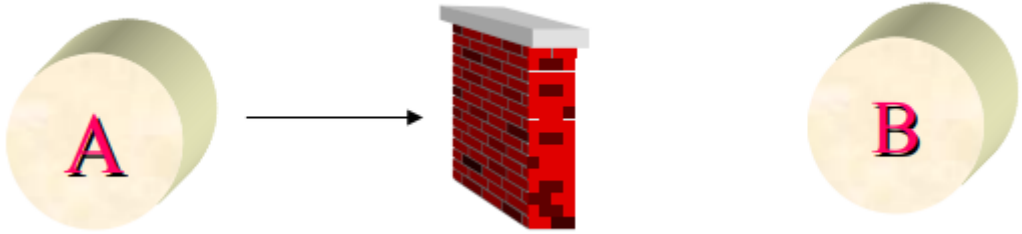


- **가로채기: 비 인가자들의 불법적인 접근에 의한 신뢰성에 대한 공격**

00_보안공격- 보안공격의 유형

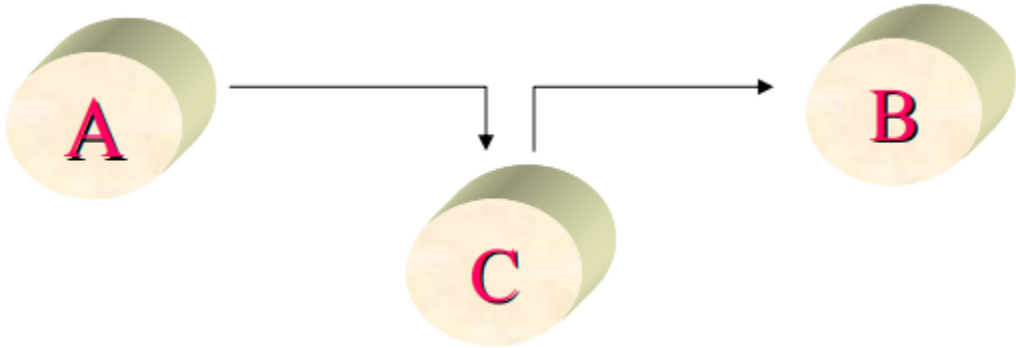
❖ 적극적 공격

- 허가 받지 않은 상태에서 파일의 삭제, 추가, 변경, 조작 등을 시도하는 공격으로 악의적 의도를 가진 이가 메시지를 조작하는 공격방식
- Ex) 방해(가용성), 수정(무결성), 재전송, DDoS → 스푸핑, 세션하이재킹 등

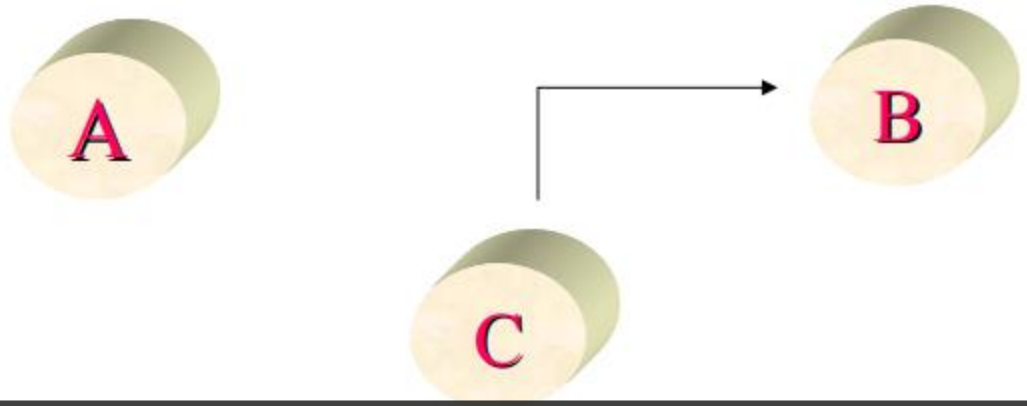


- **방해: 시스템의 일부가 파괴되거나 사용할 수 없는 경우로 가용성에 대한 공격**

00_보안공격- 보안공격의 유형



- 불법수정: 비인가자들의 불법적인 접근 뿐만 아니라 불법적인 변경에 의한 무결성에 대한 공격



- 위조: 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격

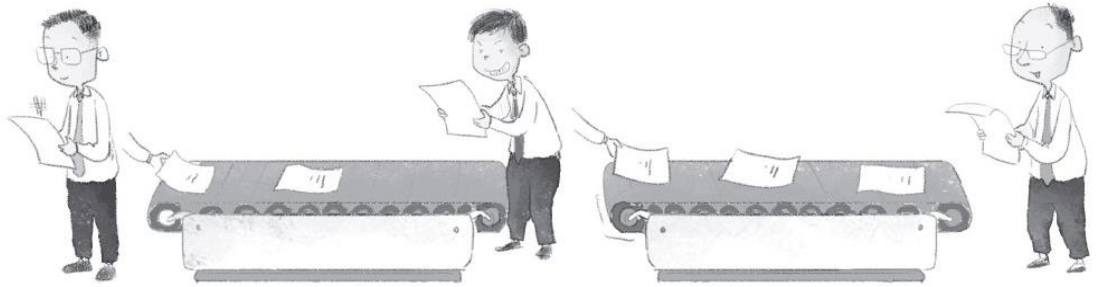
01_스니핑- 스니핑에 대한 이해

❖ 스니핑

- sniff의 사전적 의미 : 코를 킁킁거리다
- 수동적(Passive) 공격 : 공격할 때 아무것도 하지 않아도 충분하기 때문
- 스니퍼: 스니핑을 하는 도구나 인물

❖ 스니핑의 개념

- 도청(Eavesdropping)과 엿듣기가 스니핑
- 전화선이나 UTP에 탭핑(Tapping)해서 전기 신호를 분석하여 정보를 찾아냄.
- 전기 신호(Emanation)을 템페스트(Tempest) 장비를 이용해 분석하는 일



- 네트워크 측면에서 네트워크 상에서 돌아다니는 트래픽을 몰래 엿보는 행위로 기밀성을 해치는 기법

01_스니핑- 스니핑에 대한 이해

❖ 프러미스큐어스 모드(Promiscuous Mode)

- MAC 주소와 IP 주소에 관계없이 모든 패킷을 스니퍼에게 넘겨주는 것
- 리눅스나 유닉스 등의 운영체제에서는 랜 카드에 대한 모드 설정이 가능
- 윈도우에서는 스니핑을 위한 드라이버를 따로 설치
- 스니핑을 하려면 좋은 랜 카드가 필요

❖ 바이패스 모드(Bypass Mode)

- 패킷에 대한 분석까지 하드웨어로 구현되어 있는 랜 카드
- 기가바이트(GByte) 단위의 백본 망에서 스니핑을 하기 위한 장비로 고가임.

❖ 스니핑 대응책

- 스니퍼 탐지 (PING, ARP, DNS, 유인)
- 암호화

02_스푸핑- 스푸핑 공격에 대한 이해

❖ 스푸핑(Spoofing)

- '속이다'는 의미
- 인터넷이나 로컬에서 존재하는 모든 연결에 스푸핑 가능
- 정보를 얻어내기 위한 중간 단계의 기술로 사용하는 것 외에 시스템을 마비 시키는 데 사용할 수도 있음.

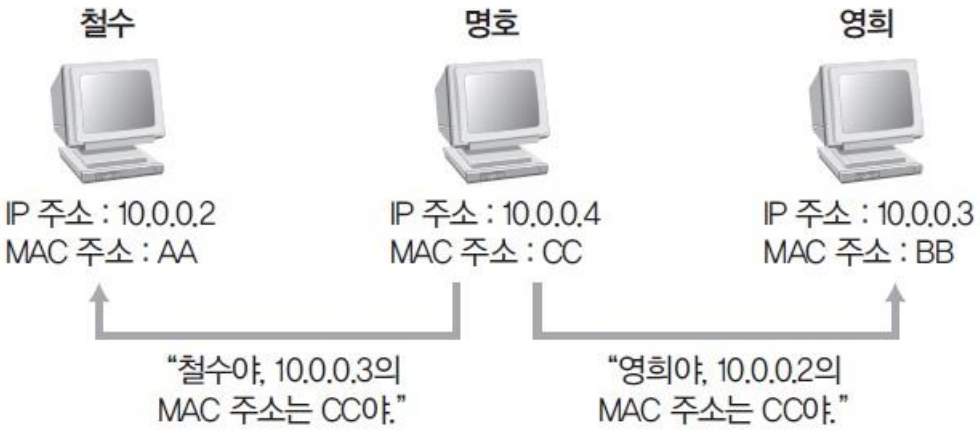
❖ 스푸핑 공격 대비책

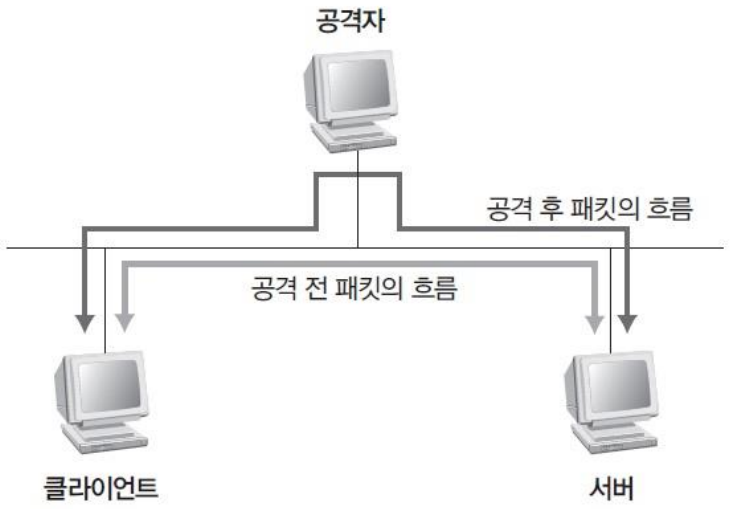
- 관리하는 시스템의 MAC 주소를 확인하여 테이블로 만들어 둠.
- 브로드캐스트 ping을 네트워크에 뿌려 그에 답하는 모든 시스템에 대한 MAC 주소 값을 시스템 캐시에 기록함.
- arp -a로 현재 IP 주소 값과 MAC 주소의 대칭 값 비교하여 엉뚱한 MAC 주소로 맵핑되어 있는 항목을 확인

02_스푸핑- 스푸핑에 대한 이해

❖ ARP 스푸핑

- MAC 주소를 속이는 것(2계층에서 작동해 공격 대상이 같은 랜에 있어야 함.)





호스트 이름	IP 주소	MAC 주소
철수	10.0.0.2	AA
영희	10.0.0.3	BB
명호	10.0.0.4	CC

02_스푸핑- 스푸핑에 대한 이해

IP 스푸핑

- IP 주소를 속이는 것

- 최근에는 계정의 패스워드가 같아야만 패스워드를 묻지 않도록 변경되었고, SSH를 사용하도록 권고하기 때문에 IP 스푸핑 공격이 이루어지지 않음.

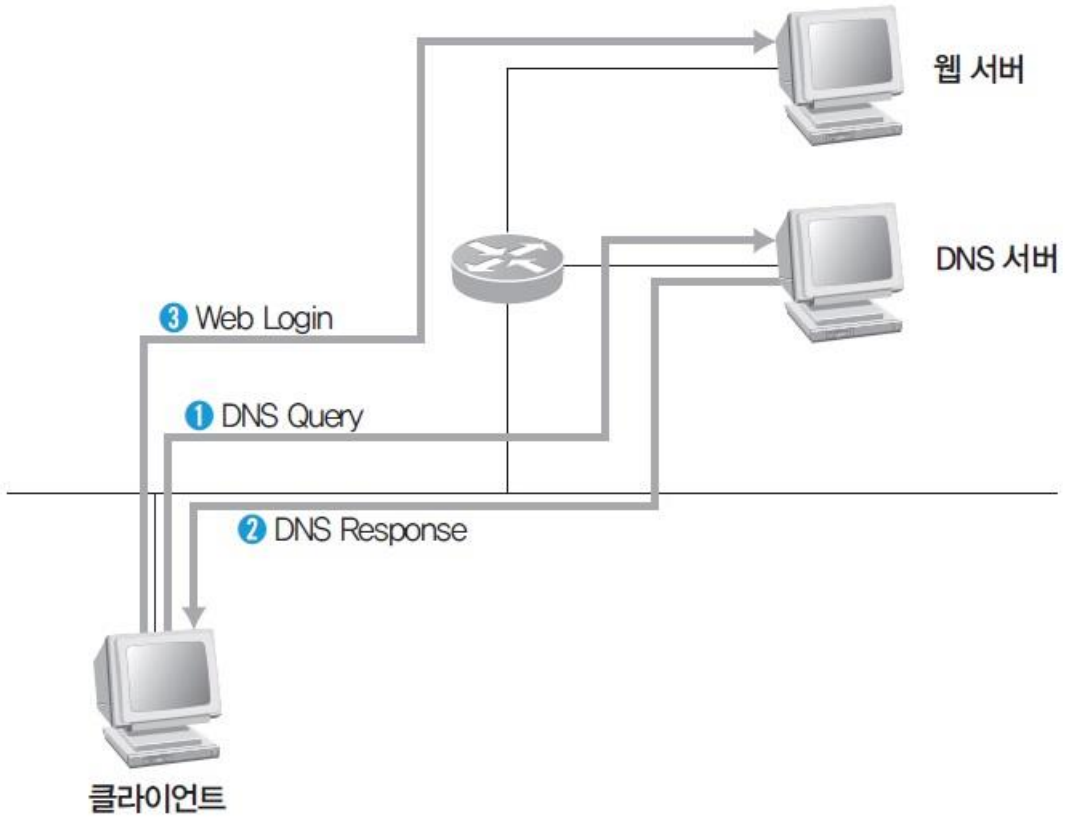
IP 스푸핑의 보안 대책

- 가장 좋은 보안 대책은 트러스트를 사용하지 않는 것
- 트러스트를 사용해야 한다면 트러스트된 시스템의 MAC 주소를 static으로 지정

02_스푸핑- 스푸핑에 대한 이해

❖ DNS 서비스

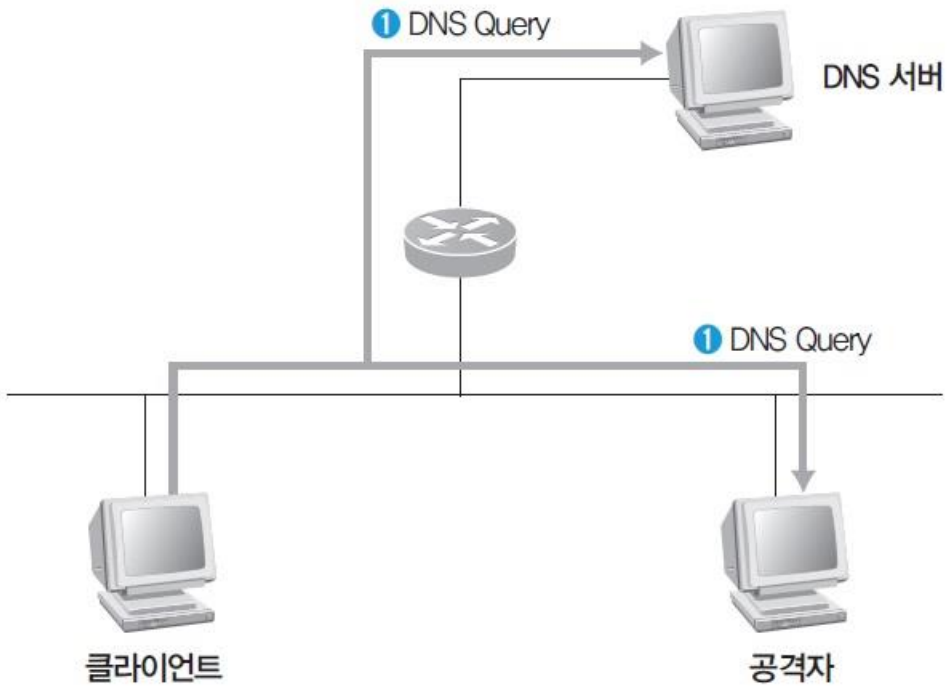
- 정상적인 DNS 서비스



02_스푸핑- 스푸핑에 대한 이해

❖ DNS 스푸핑

① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인(ARP 스푸핑과 같은 선행 작업이 필요)



❖ DNS 스푸핑

② DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 위조된 DNS Response 패킷을 클라이언트에게 보냄.

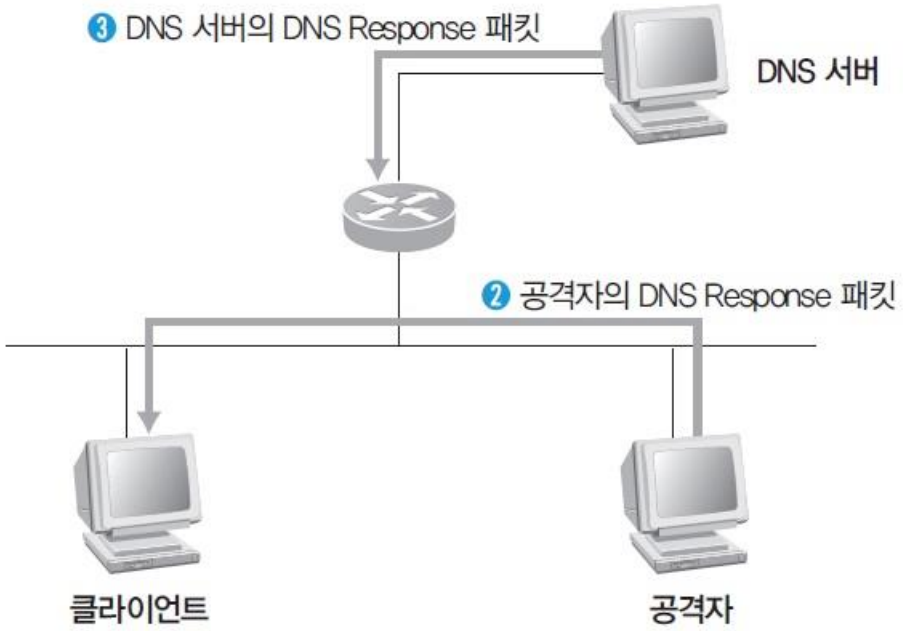


그림 7-20 공격자와 DNS 서버의 DNS Response

❖ DNS 스푸핑

③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고 웹에 접속

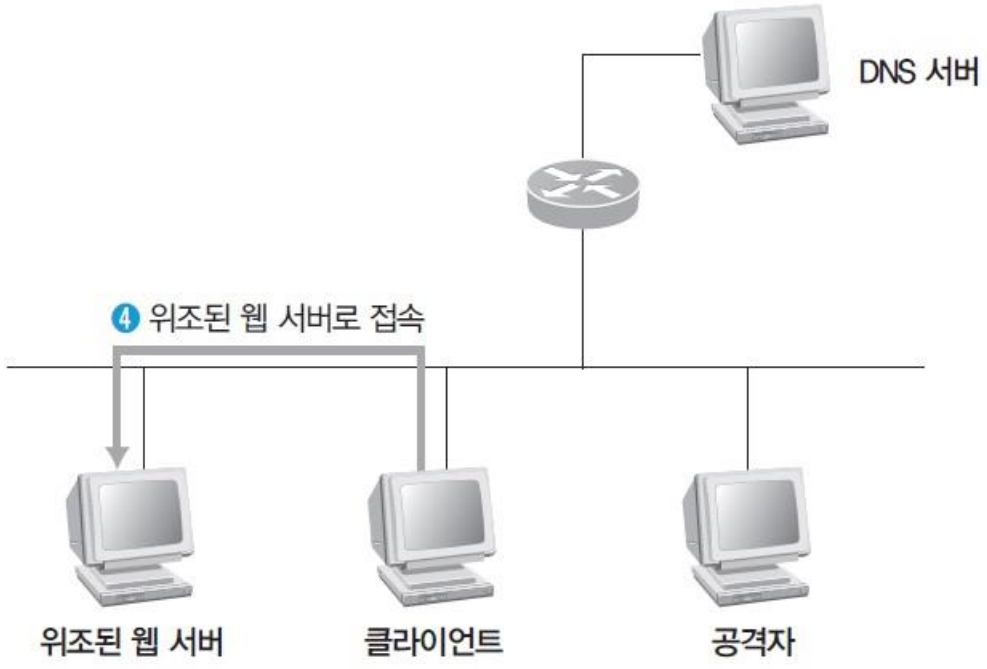
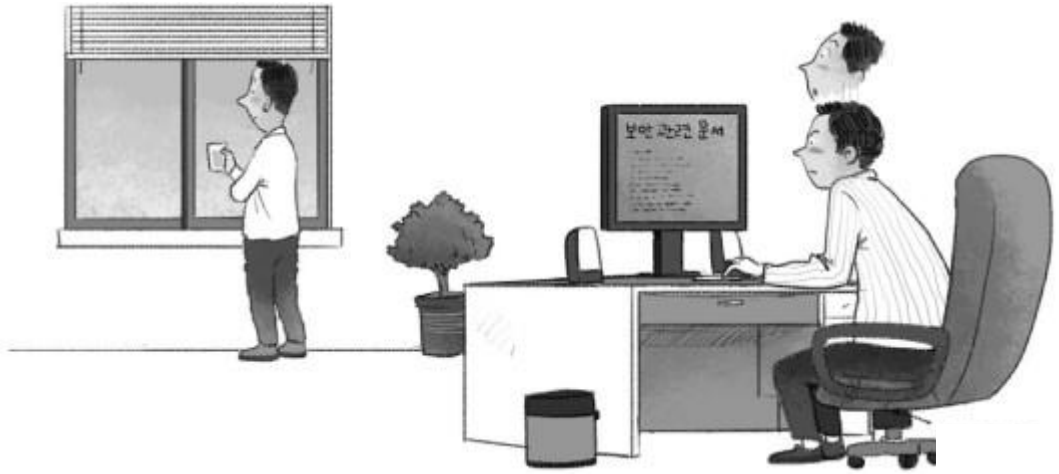


그림 7-21 공격 성공 후 도착한 DNS Response

03_세션 하이재킹 공격

❖ 세션 하이재킹(Session Hijacking)

- '세션 가로채기'라는 의미
- 세션 : 사용자와 컴퓨터, 또는 두 컴퓨터 간의 활성화 상태
- 두 시스템 간 연결이 활성화된 상태, 즉 로그인(Login)된 상태를 가로채는 것을 뜻함.



- 네트워크 측면에서 네트워크 상에서 돌아다니는 트래픽을 몰래 엿보는 행위로 기밀성을 해치는 기법

04_MITM 공격

MITM(Man In The Middle) 공격

- 글자 그대로 누군가의 사이에 끼어드는 것
- 중간자 공격은 통신을 연결하는 두 사람 사이에 침입하여 두 사람은 연결되었다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후에 다른쪽으로 전달한다.

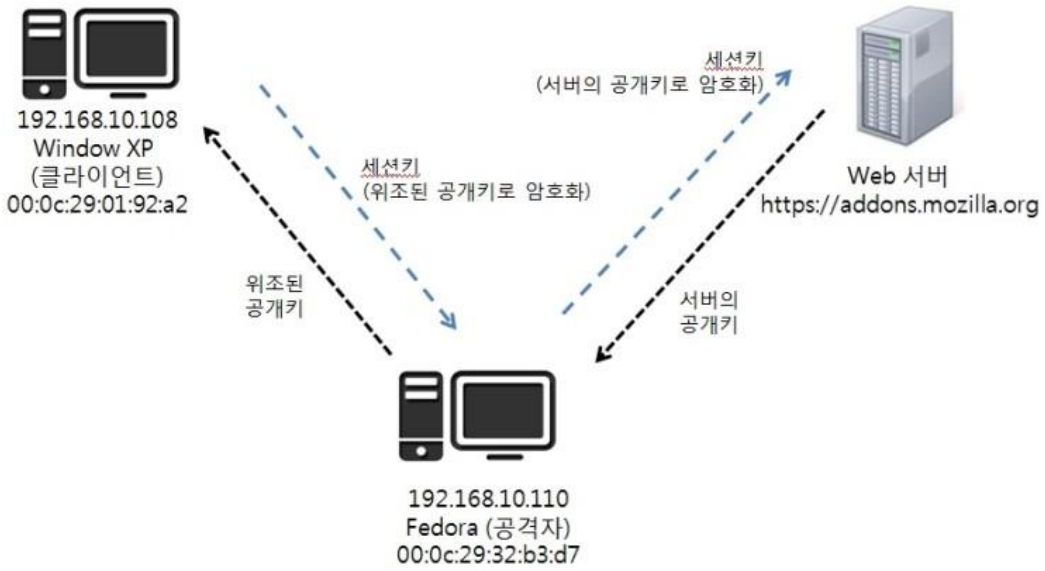
1. 공격자 (Fedora)의 IP는 192.168.10.110 MAC 주소는 00-0c-29-32-b3-d7 이다.

2. 클라이언트 (Window XP)의 IP는 192.168.10.108 MAC 주소는 00-0c-29-01-92-a2 이다.

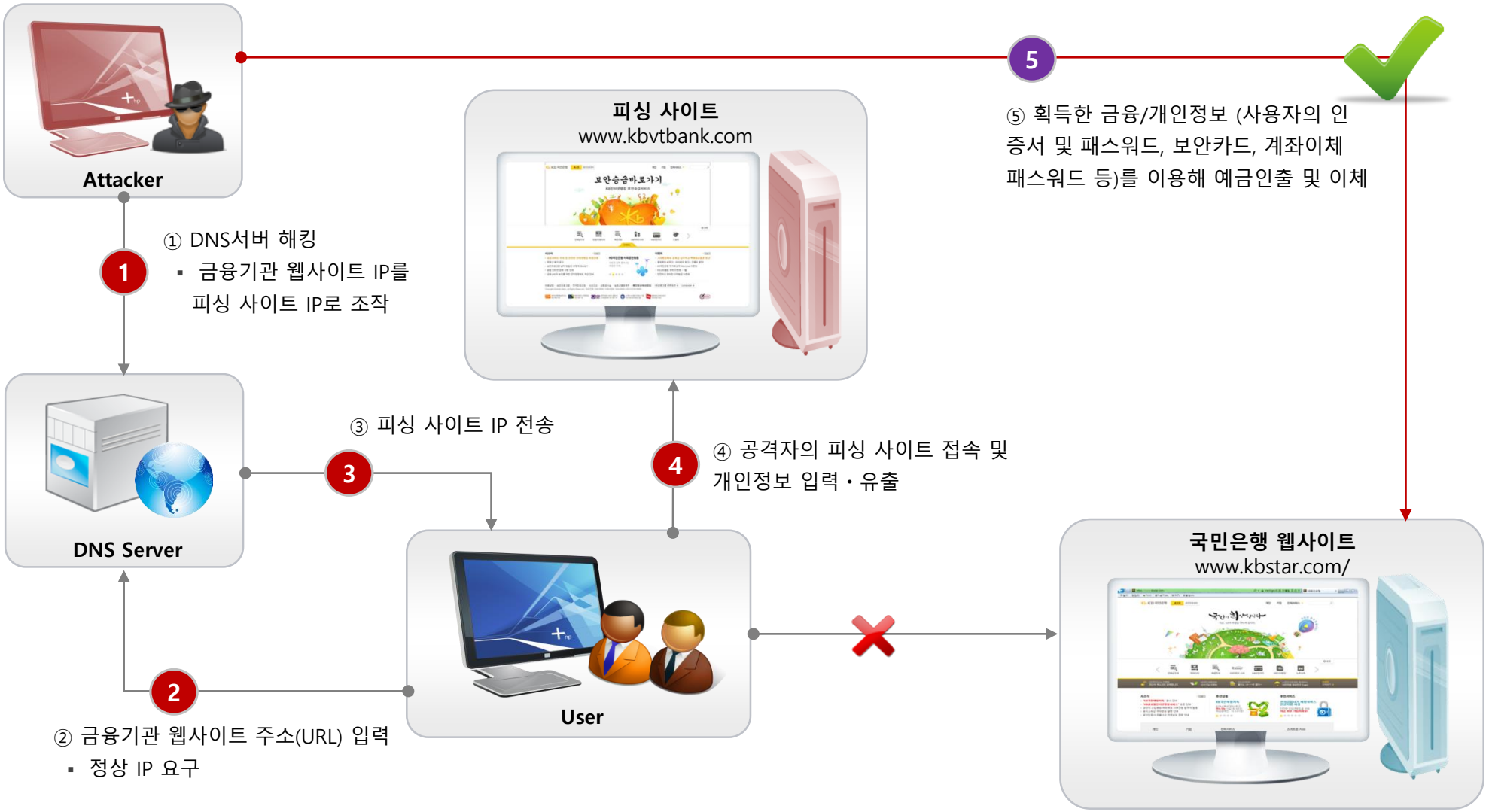
3. Web 서버는 클라이언트가 SSL을 통해 접속하려는 Web 사이트이다.

4. 공격자는 클라이언트에게 변조 된 ARP 패킷을 보내 ARP 스푸핑 공격과 DNS스푸핑 공격을 하고 클라이언트에게 위조된 공개키를 보내 세션키를 탈취한다.

5. 공격자는 게이트웨이에게 변조 된 ARP 패킷을 보내 ARP 스푸핑 공격을 통해 서버의 공개키를 탈취한다. 공격자는 클라이언트가 공격자에게 보낸 세션키를 서버의 공개키로 암호화하여 서버에게 보낸다.



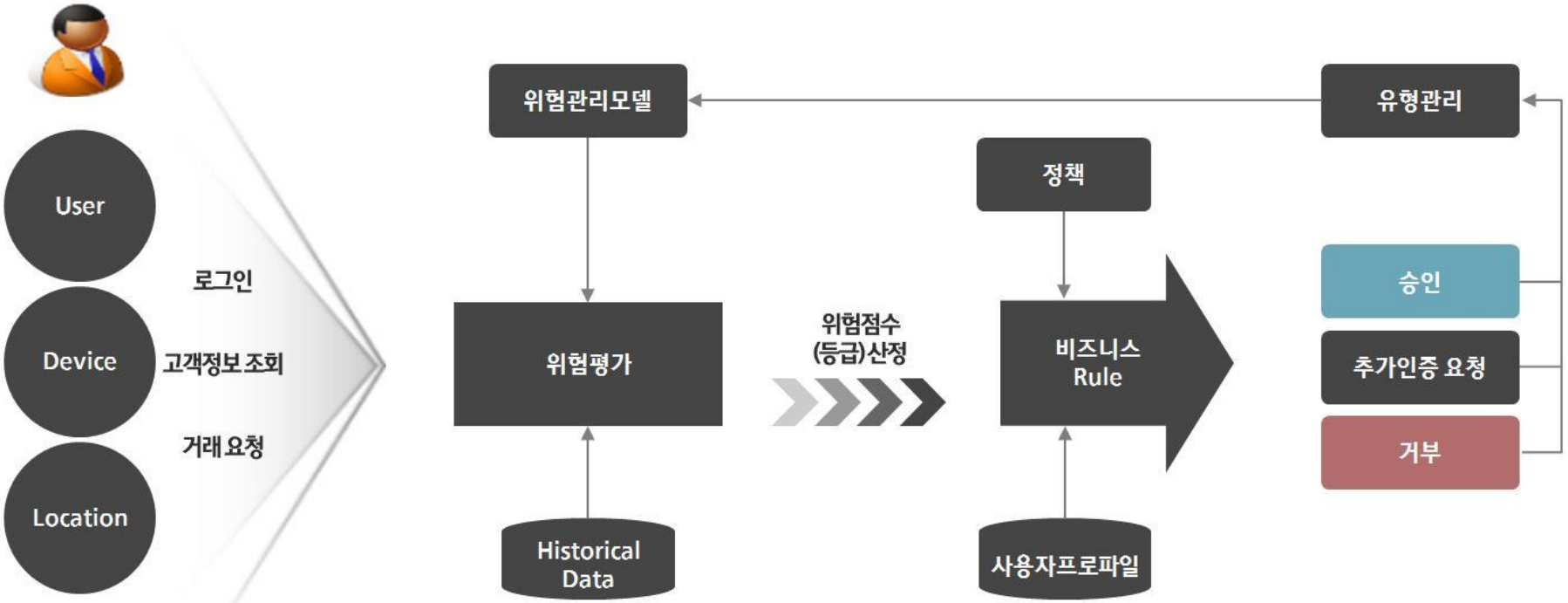
04_금융권 피싱/파밍 보안사고 절차



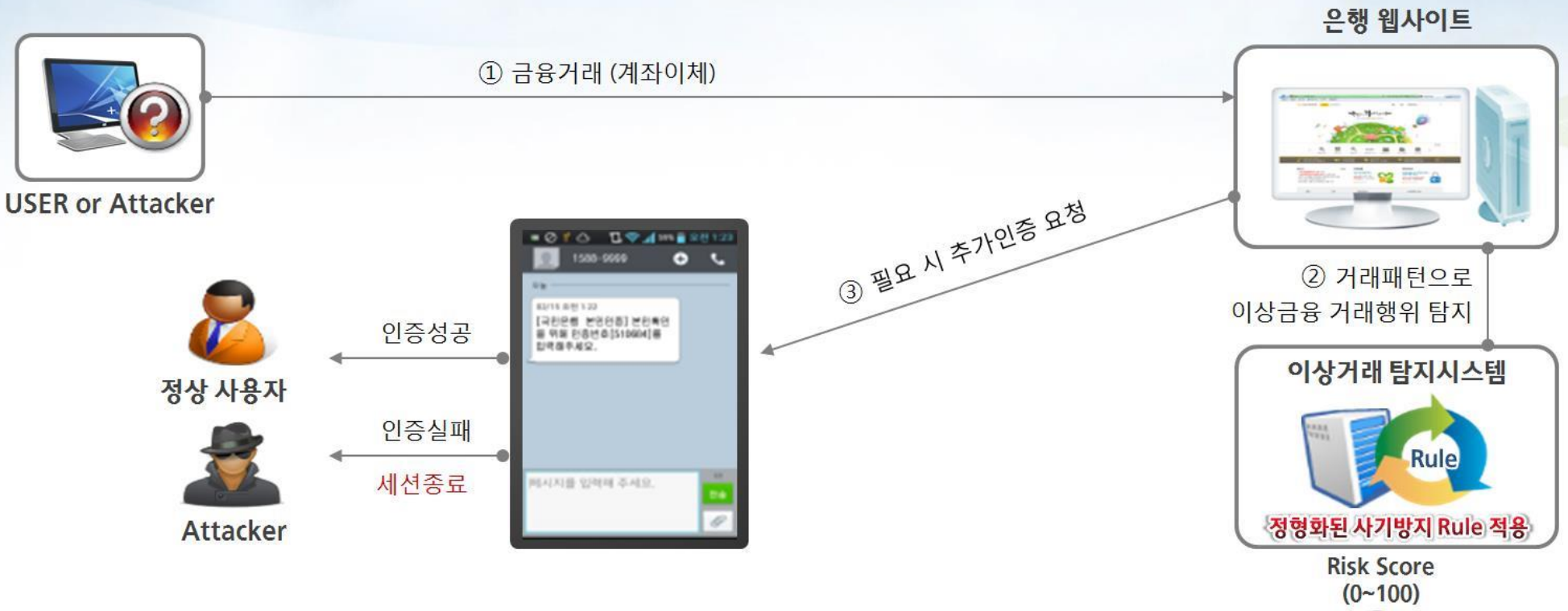
진정한 의미의 인증체계 수립 방안 – 사용자 이상행위 탐지 프로세스

Risk-based Work Flow를 기반한 이상행위 탐지 프로세스 수립

사용자의 정상적인 업무 요청에 대한 패턴을 분석, 위험을 평가하는 지표로 활용하여 의심행위 탐지에 대한 신뢰도를 향상



금융 이상거래 탐지 – RISK 기반 인증



한국의 IT 보안 새출발

- 공인인증서 오해와 진실

Pre-View : 암호기술 배경

컴퓨터와 네트워크의 발전으로
전자적 정보를 광범위 하게 사용하게
됨으로써 정보보호를 위한 암호화 기술
필요

공개키 기반 기술(Public Key Infrastructure)

- 공개키 암호기술을 통한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템
- 국내 대표적인 공인인증서

공개키 암호기술

- 암호화/복호화에 다른 키를 사용하는 방식
- 키 분배 및 관리의 용이
- 속도가 느리고 구축비용 증가

$key = 2n$

Pre-View : 공인인증서의 현황과 문제점

1998년 은행에서 PKI 방식의 사설 인증서

2002년 인터넷 뱅킹을 공인인증서 기반으로 전환

1999년에 공인 인증서 등장

공인인증서의 한계

- 사용의 불편함: 공인인증서의 발급/사용 절차 복잡, 제한된 저장 매체 사용
- 보안의 취약점: 단순한 파일형태로 복제 가능, 저장 경로 동일, 인증서 해킹
- 전자문서 활성화와 전자거래의 걸림돌: ActiveX 기반

목차 *Contents*

한국의 IT 보안 새출발
- 공인인증서 오해와 진실

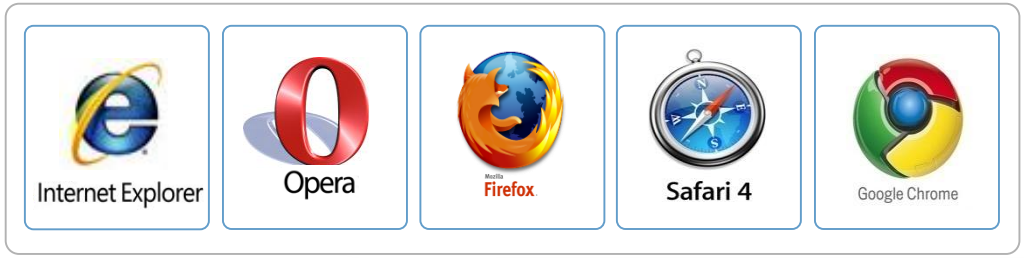
공인인증서 어떻게 시작 되었나

인터넷이란 환경은 거래 당사자간의 비 대면성 특징으로 인해 보안의 여러 가지 문제가 발생 가능하다. 금융, 전자상거래 등 민감한 정보를 안전하게 전달하기 위해 '고강도'암호화 기술이 필요

❖ 1999년 ETRI 128bit 길이의 키를 사용한 대칭 암호화 알고리즘(SEED) 개발에 성공

독자 개발한 SEED 사용을 위해서는

웹 브라우저



별도의 프로그램
(플러그인)

BUT

'간명한 해법'이 위험을 초래

인터넷 환경에서의 보안?

- 1999년도 개발한 128bit의 암호기술이 현재에는 보안 강도 면에서 이제 저급한 수준으로 전락 (현재 256bit의 암호화를 웹 브라우저에서 제공)
- 웹 사이트에서 내려주는 알지 못하는 프로그램에 대한 설치가 보안 위험을 초래

- 2000년 5월부터 모든 웹 브라우저들이 이미 같은 수준의 암호화 접속 기능을 기본 탑재
- 별도 프로그램을 유저의 컴퓨터에 설치해야 하는 기술은 매우 심각한 보안 위험을 초래하므로, 오히려 사용되면 안됨

한국형 공인인증 기술의 특징- 독특한 저장 위치

우리나라의 공인인증서는 NPKI라는 폴더에 저장된다. 사용자의 인증서를 이런 위치에 저장하는 경우는 전세계 유례가 없는 경우로, 다음과 같은 문제가 발생한다.

공인인증서의 저장 위치

- USB 폴더 내에 NPKI라는 폴더에 사용자의 공인인증서 저장
- 하드디스크에 저장할 경우 위치는C:₩Program Files₩NPKI폴더(윈도우XP의 경우)거나, %UserProfile%₩AppData₩LocalLow₩NPKI폴더 (윈도우 Vista 이후)

문제점

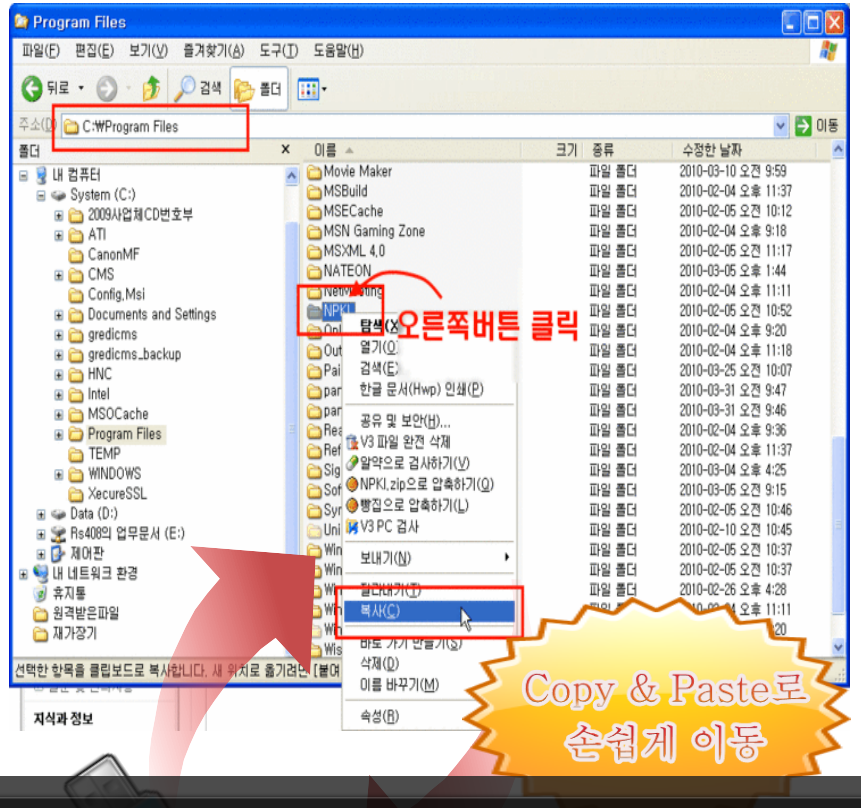
❖ 어떤 웹 브라우저도 NPKI라는 폴더에 저장된 사용자 인증서를 인식할 수 없다.
- 인식을 위해서 부가 프로그램을 사용자의 컴퓨터와 웹 서버에 설치필요

❖ 웹 서비스 제공업자들은 부가 프로그램을 국내 보안업체로부터 구입해서 사용자들에게 배포해야 한다.
- 웹 브라우저가 인식할 수 있는 위치와 방법을 사용했다면, 부가 프로그램 설치가 불필요하여 솔루션 구매도 불필요

❖ 공인인증용 부가 프로그램의 안전성을 제대로 검증할 방법이 없다.
- 은행이 프로그램의 안전성을 검증할 역량이 있는 것도 아니고, 소스가 공개된 것도 아니기 때문
- 오로지 제작 업체의 기술력과 윤리성에만 전적으로 의존 (보안 업체를 무작정 믿으라는 것)

한국형 공인인증 기술의 특징- 손쉬운 무단 복제

하드디스크에 있는 공인인증서를 USB로 복사하거나, USB에 저장된 인증서를 하드디스크에 복사할때에는 NPKI폴더를 단순히 복사해서 붙이기(Copy + Paste)로 손쉽게 이루어 진다.



공인인증서를 스마트폰에 복사하는 방법

1. 인증서가 담긴 USB를 PC에 꽂는다.
   NPKI폴더를'오른 클릭'하여 복사한다.

2. 안드로이드 폰을 PC에 연결한다.
   폰 화면 상단에 USB 아이콘이 뜨는데, 이것을 쓸어내려 스마트폰이 USB대용량 저장장치로 인식되게 선택한다. 그러면 스마트폰SD 카드 폴더들이 나타나는데, 그 중 빈 공간에 마우스를'오른 클릭'해서 조금 전에 복사해둔 NPKI 폴더를 붙여 넣는다.

   이렇게 하면 공인인증서가 스마트폰으로 복사된다.

- 공인인증서는 아무 곳으로나 마구 복사되기 때문에 암호를 입력하라는 것은 순전히'쇼'에 불과하다.
- 손쉬운 복사방법을 설명보다는 Activex를 설치하라, 8자리 인증코드를 입력하라, 주민번호를 입력하라, 비밀번호를 입력하라, QR코드를 찍으라 등의 온갖 복잡한 과정은 "보안 코스프레"를 하는 것이다.

한국형 공인인증 기술의 특징– 더 많은 부가 프로그램 설치 필요

사용자 컴퓨터에 침입이 성공되면 공격자는 사용자의 공인인증서(개인키) 파일을 손 쉽게 획득할 수 있다. 인증서 개인키 암호를 어떻게 보호할 것이냐에 모든것이 달려있다. 대표적인 예로 키보드 보안 프로그램 설치를 강제로 하는 금융기관을 들 수 있다.

❖ 인증서 암호는 유저가 정하는 것이다.

- 대부분 유저들은 다른 여러 계정에서 사용하는 암호와 인증서 암호를 같이 정해두고 사용.
- 유저들이 다른 계정에서 입력하는 암호는 유출위험 높음.

- 금융기관들이 아무리 키보드 보안 프로그램 설치를 강제해도 그 실효성은 기대할 것이 못 된다.
- 금융기관들이 유저들에게 인증서 암호는 다른 어떤 계정 암호와도 다르게 정해두고 사용하라고 계몽하긴 하지만, 실제로 이런 권고를 실천하는 유저들의 비율이 높기를 기대 할 수는 없다.

법률의 오해

공인인증서의 기술적 취약점에도 불구하고, 국내 보안업계는 전자서명의 '법적효력'을 거론하면서 공인인증서 사용이 법적으로 불가피한 것처럼 주장하기도 한다.

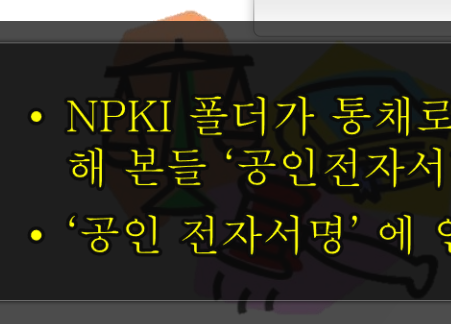
전자서명법 제 3조 제 2항

② 공인 전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명 된 후 그 내용이 변경되지 아니하였다고 추정한다.

※ 여기서'전자서명생성정보'란 인증서'개인키'를 말함.

'공인 전자서명'으로 인정받으려면 다음 요건을 반드시 구비

가. 전자서명생성정보가 가입자에게 유일하게 속할 것
나. 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것
[이하 생략]



- NPKI 폴더가 통채로 복사되고 인증서 암호가 유출된 상황이라면 그런 공인인증서로 아무리 전자서명을 해 본들 '공인전자서명'으로 인정 받을 수는 없다.
- '공인 전자서명' 에 인정되는 '추정력'이라던가 ,'부인방지'효력이란 것은 아예 거론할 여지가 없게 된다.

극복방안

부가 프로그램을 설치해야만 하는 공인인증서 때문에 한국의 유저들은“보안경고창이 나타나면 반드시‘설치’를 눌러 진행하십시오”라는 안내를 받아왔다. 13년 넘게 계속된 공인인증/ActiveX에 의존한 국내 보안 체제의 소프트 랜딩(soft landing)을 고민해야 할 때다.

극복방안

❖ 공인인증서는‘선택(option) 사항’으로 전환

더 이상 정부가 특정 보안 기술 사용을‘강요’해서는 안 된다. 다양한 보안기술이 활발히 경쟁할 수 있어야 보안 기술이 발달한다

❖ 공인인증서‘저장 위치’는 키 저장소(keystore) 사용

부가 프로그램(ActiveX 등)을 설치 하지 않아도 공인인증서를 이용할 수 있다

❖ 공인인증서 로그인은 유저가 원할 경우에 선택할 수 있도록 옵션(option)으로 제공

공인인증서 사용을 강제하지 않고 ‘선택사항’으로 전환하는 것이
지금 우리에게 시급하게 필요한, 유일한 해결책이다.